Everything You Always Wanted to Know About Maturity Models

Dr. Nader Mehravari, MBCP, MBCI

CERT Resilience Management Team
Software Engineering Institute
Carnegie Mellon University
http://www.cert.org/resilience/

January 23, 2014

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
23 JAN 2014	**N/A**	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Everything You Always Wanted to Know About Maturity Models	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Mehravari /Nader	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Carnegie Mellon Software Engineering Institute, 4500 Fifth Ave, Pittsburgh, PA 15213	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**40**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

Outline

Setting the Stage

- The need for “measuring” operational activities & their effectiveness
- Are we doing the right things?
- Are we using the right tools to measure?
- Are we measuring the right things?

ABCs of Maturity Models

- What are Maturity Models?
- Types of Maturity Models
- Examples of Maturity Models

Closing Thoughts

- A few cautions
- Determining when and which type to use

Setting the Stage

- The need for “measuring” operational activities & their effectiveness
- Are we doing the right things?
- Are we using the right tools to measure?
- Are we measuring the right things?

Today's Operating Environment

Rapid changes in technology and its application in a wide range of industries.

Introduction of many new systems, business processes, markets, risks, and enterprise approaches.

Many immature products and services being consumed by enterprises that themselves are in a state of change.

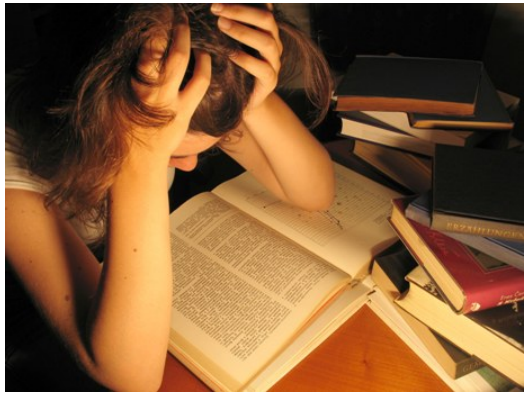
Challenges at Hand

How can you tell if you are doing a good job of managing these changes?

How best to monitor your progress on an ongoing basis?

How do you manage the interactions of systems and processes that are continually changing?

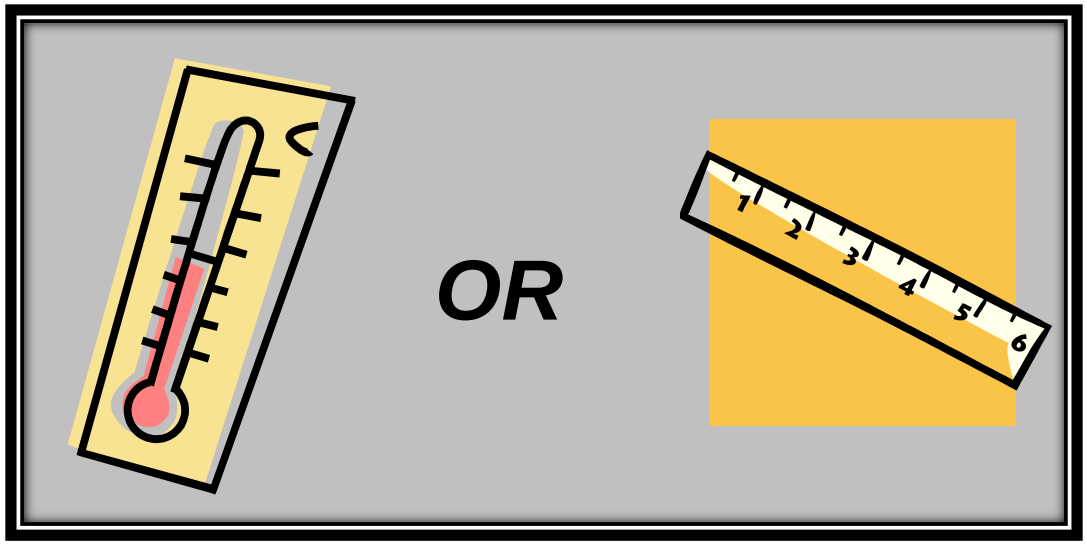
How do poor processes impact interoperability, safety, reliability, efficiency, and effectiveness?



Which tool should I use?

Your organization wants to know **SOMETHING** about your mission operation:

- How **EFFECTIVE** are we?
- Do we have the right **SKILLS** and **CAPABILITIES**?
- Do we have the right **TECHNOLOGIES**?



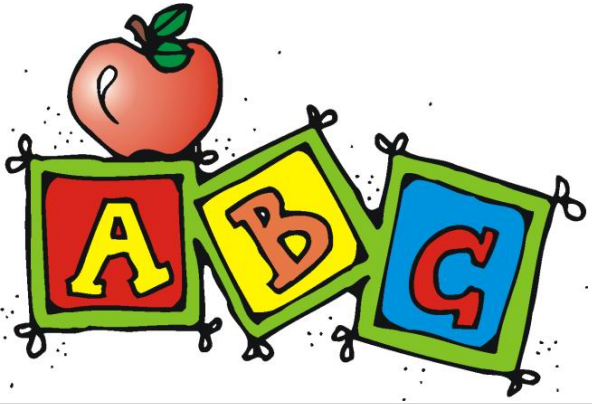
Observation

Do maturity models measure the right thing?

- **May not measure what you think it measures**
  - Practice maturity vs. organizational maturity?
- **May give you inaccurate data on which to base decisions**
  - Process performance vs. product performance?
- **Can increase cost but reduce benefit**
  - An improved process may not result in compliance
- **May provide a false sense of confidence**
  - A robust process may not stop all malware

ABCs of Maturity Models

- What are Maturity Models?
- Types of Maturity Models
- Examples of Maturity Models

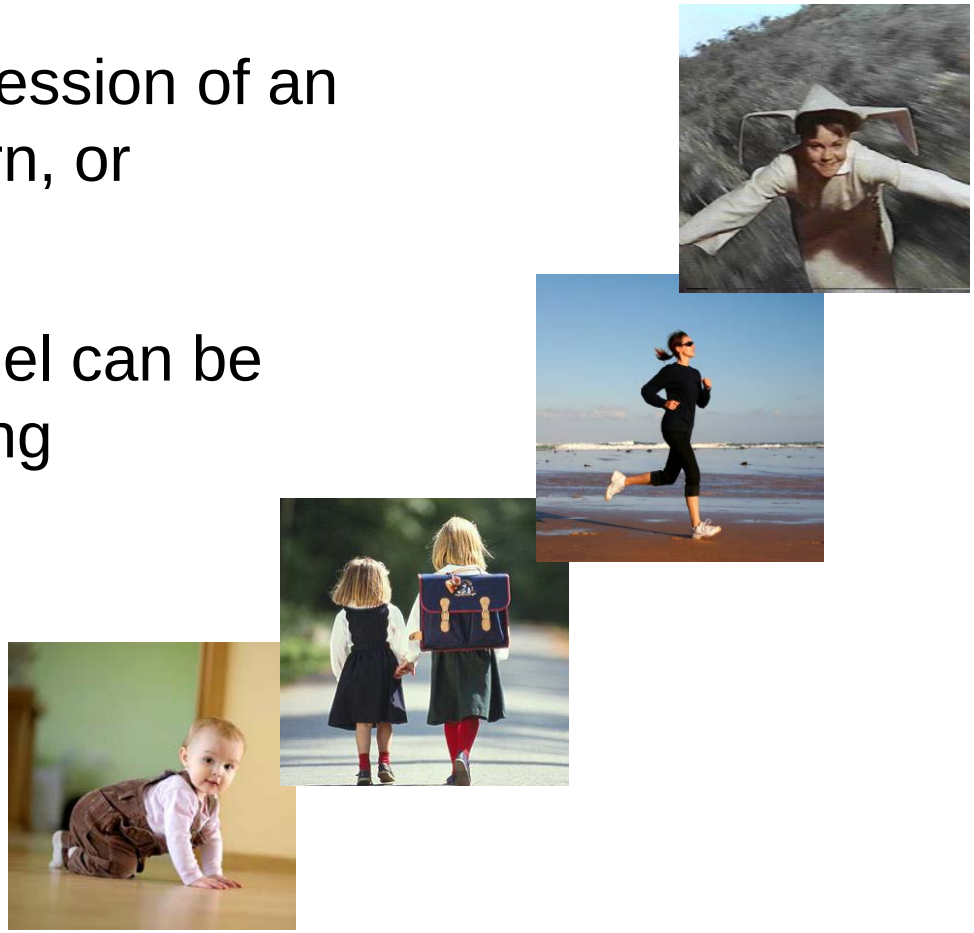


Maturity Model Defined

An organized way to convey a path of experience, wisdom, perfection, or acculturation.

Depicts an evolutionary progression of an attribute, characteristic, pattern, or practice.

The subject of a maturity model can be objects or things, ways of doing something, characteristics of something, practices, controls, or processes.



Maturity Models Provide…

Means for assessing and benchmarking performance

Ability to assess how a set of characteristics have evolved

Expression of body knowledge of best practices

Identification of gaps and improvement plans

Roadmap for model-based improvement

Demonstrated results of improvement efforts

Common language or taxonomy

Key Components of a Maturity Model

Levels

- The measurement scale
- The transitional states

Domains

- Logical groupings of like attributes into areas of importance to the subject matter and intent of the model
- Logical groupings of like practices, processes, or good things to do

Attributes

- Core content of the model arranged by domains and levels
- Typically based on observed practices, standards, or expert knowledge

Diagnostic Methods

- For assessment, measurement, gap identification, benchmarking

Improvement Roadmaps

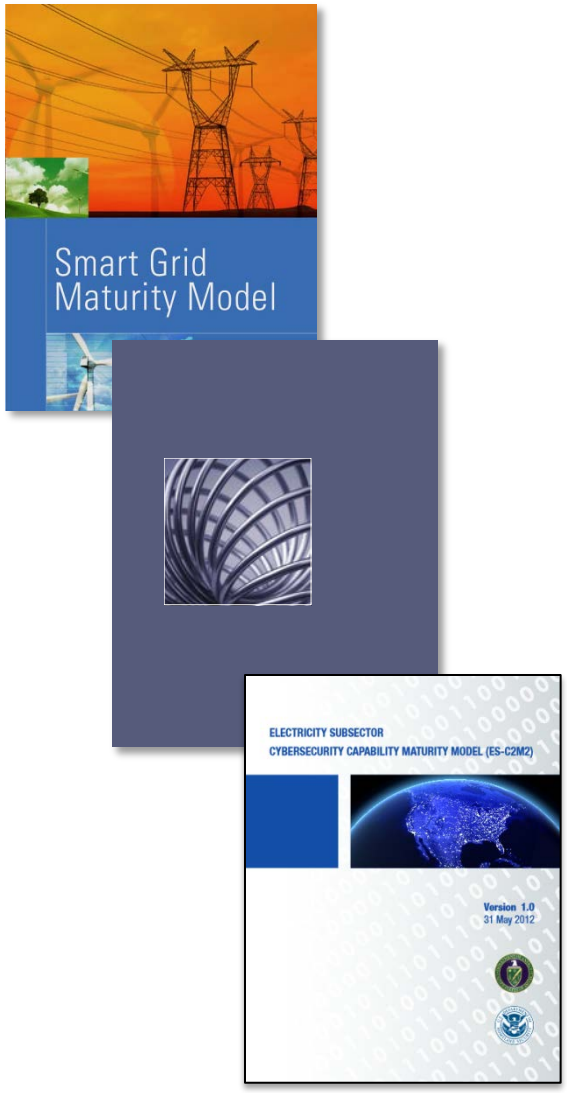
- To guide improvement efforts (e.g., Plan-Do-Check-Act)

Types of Maturity Models

There are three types of maturity models

- Progression Maturity Models
- Capability Maturity Models (CMM)
- Hybrid Maturity Models

One or more may be appropriate for your particular needs



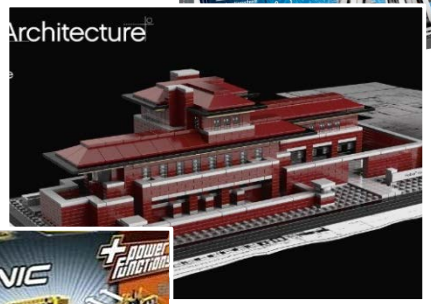
Not all maturity models are CMMs

Progression Maturity Models

Simple progression or scaling of an attribute, characteristic, pattern, or practice

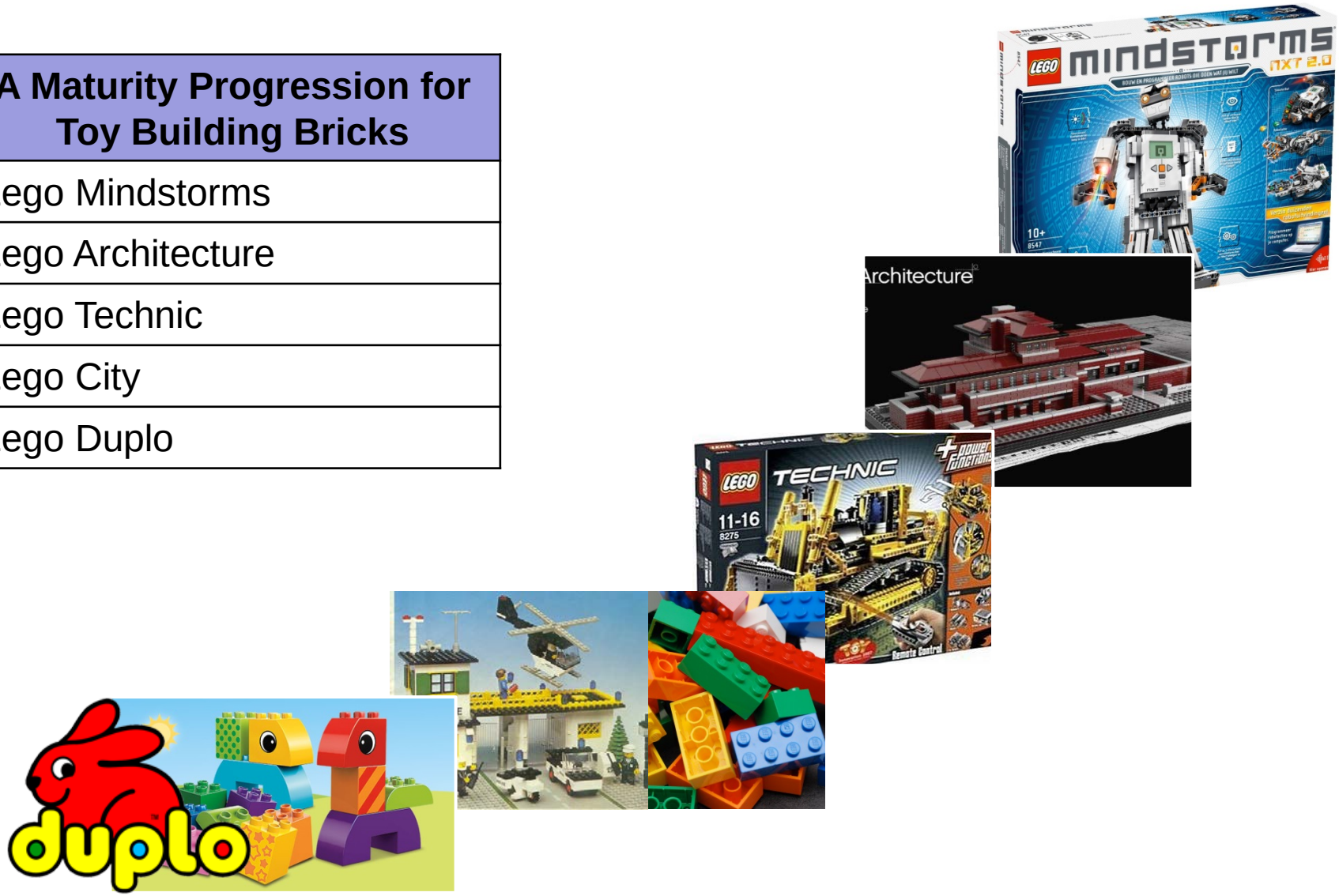
Levels describe higher states of achievement, advancement, completeness, or evolution

Levels can be arbitrary as agreed upon by users, industry, etc.



Progression Maturity Models - Example

A Maturity Progression for Toy Building Bricks
Lego Mindstorms
Lego Architecture
Lego Technic
Lego City
Lego Duplo



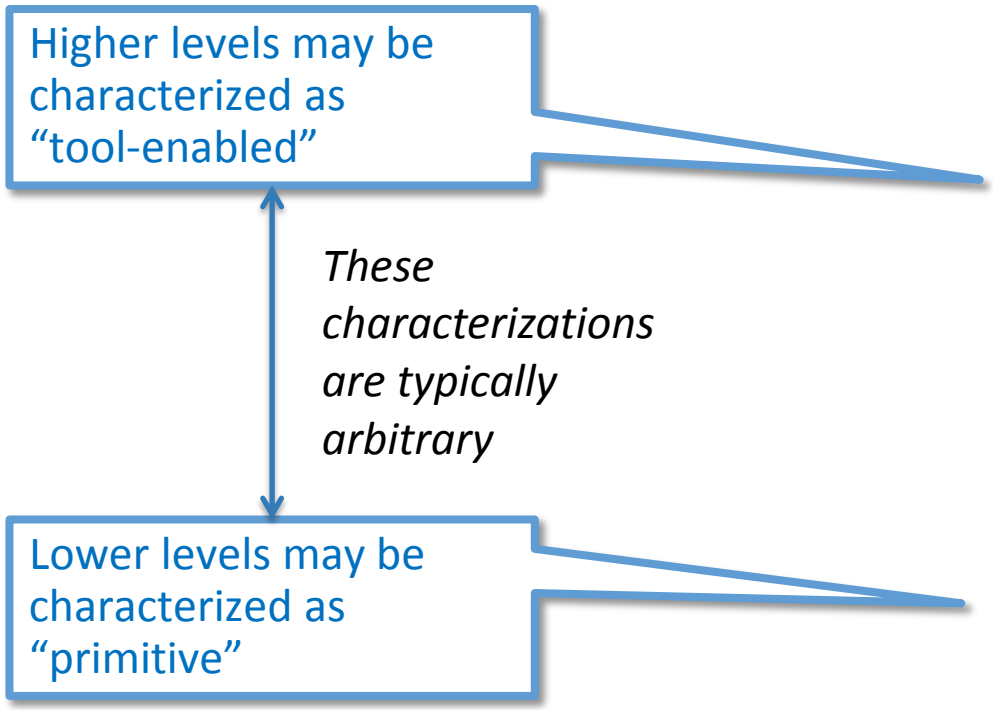
Progression Maturity Models - Example

A Maturity Progression for Human Mobility
Fly
Sprint
Run
Jog
Walk
Crawl

A Maturity Progression for Authentication
Three-factor authentication
Two-factor authentication
Addition of changing every 60 days
Use of strong passwords
Use of simple passwords

Progress does not necessarily equate to maturity

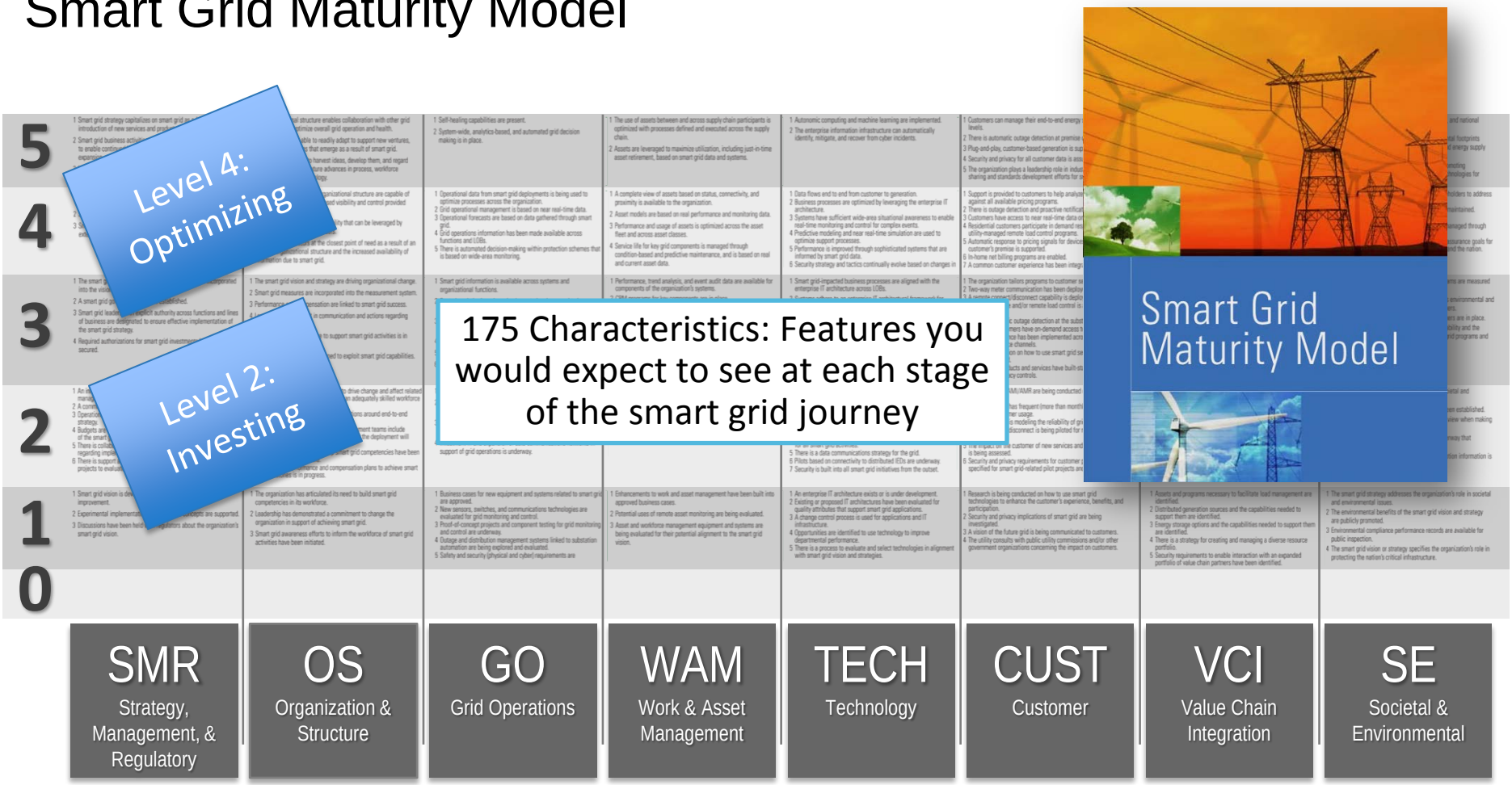
Progression Maturity Models - Example



A Maturity Progression for Counting
Computer
Calculator
Adding machine
Slide rule
Abacus
Pencil and paper
Sticks/Stones
Fingers

Progression Model Example: SGMM

Smart Grid Maturity Model



Benefits and Limitations of Progression Models

Benefits

- Provides a transformative roadmap
- Simple to understand and adopt; low adoption cost
- Easy to recalibrate as technologies and practices advance

Limitations

- Levels are arbitrarily defined and may be meaningless
- Achieving higher levels does not necessarily translate into “maturity”
- Often confused with CMMs—thus users inaccurately project traits of CMMs on progression models

Capability Maturity Models (CMM)

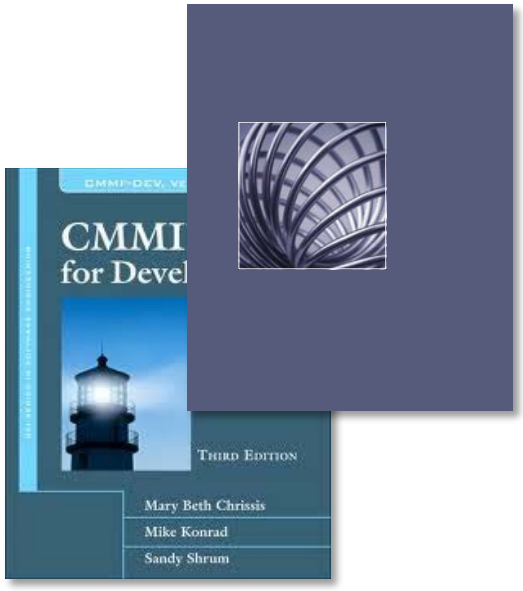
A more complex instrument

Characterizes

- the maturity of processes
- the degree to which processes are **institutionalized**
- the degree to which the organization demonstrates process maturity
- the maturity of the **culture** of the organization

Levels reflect the degree to which a particular set of practices have been institutionalized

- Institutionalized processes are more likely to be retained during times of stress.



What do these organizations have in common?

Customer Happiness

Chain of Command
Unit Cohesion
Regulations

Strong Culture

Customer Service

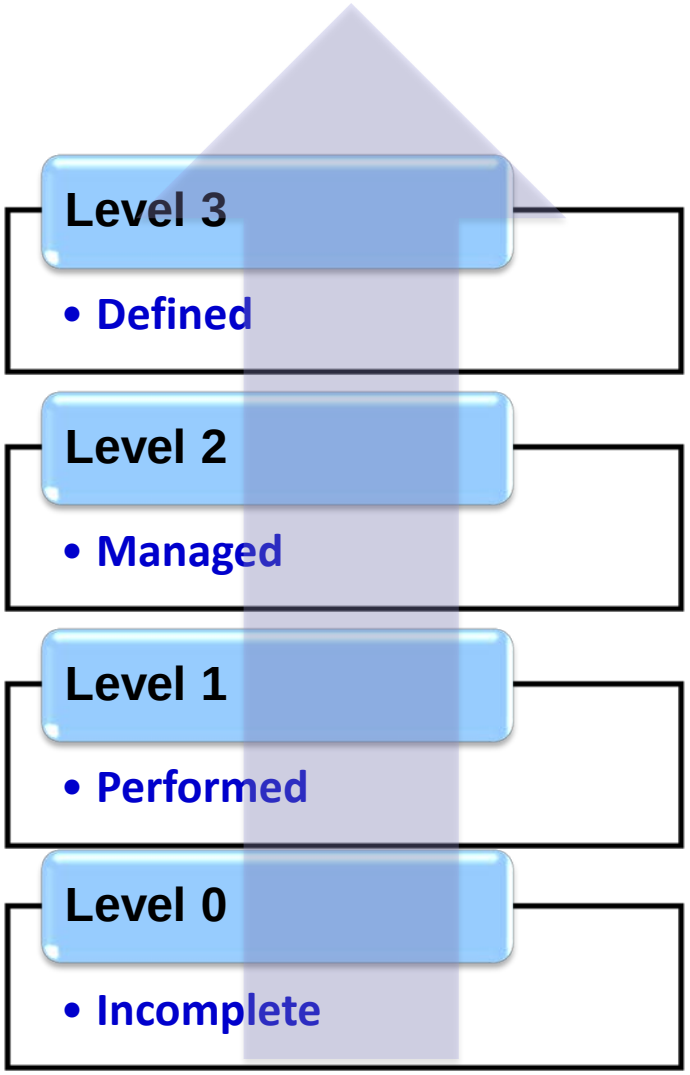
Tradition
Protection

CMM Levels – An Example

Processes are acculturated, defined, measured, and governed

Practices are performed

Practices are incomplete



Higher degrees of institutionalization translate to more stable processes that

- *are repeatable*
- *produce consistent results over time*
- *are retained during times of stress*

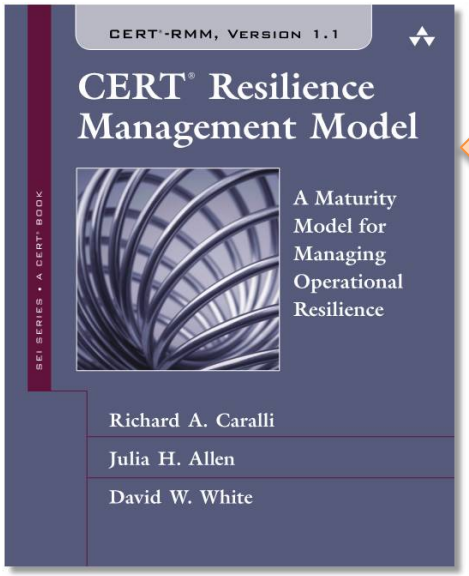
Examples of CMM Levels

Example 1
Optimized
Quantitatively Managed
Defined
Managed
Ad hoc

Example 2
Externally integrated
Internally integrated
Managed
Performed
Initiated

Example 3
Shared
Defined
Measured
Managed
Planned
Performed but ad hoc
Incomplete

Capability Maturity Model Example: CERT-RMM



Framework for managing and improving operational resilience

http://www.cert.org/resilience/

"…an extensive super-set of the things an organization could do to be more resilient."

- CERT-RMM adopter

CMM Example: CERT-RMM

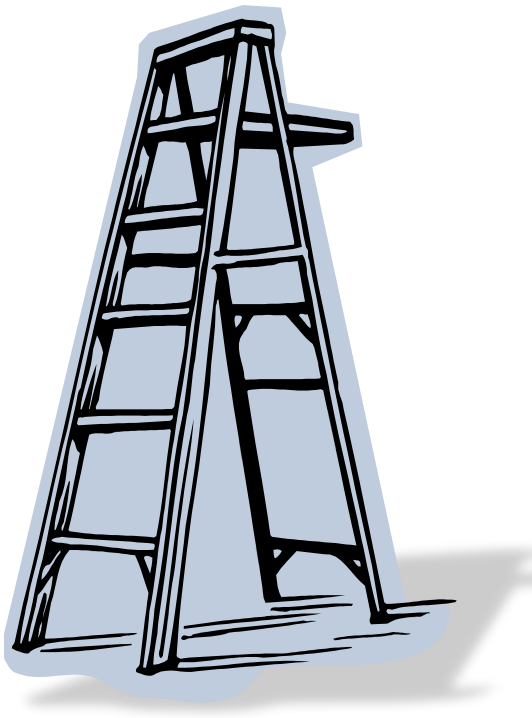
CERT-RMM Process Areas (Domains)

Access Management	Measurement and Analysis
Asset Definition and Mgmt.	Monitoring
Communications	Organizational Process Focus
Compliance	Organizational Process Definition
Controls Management	Organizational Training & Awareness
Enterprise Focus	People Management
Environmental Control	Resilience Requirements Development
External Dependencies	Resilience Requirements Mgmt.
Financial Resource Mgmt.	Resilient Technical Solution Engr.
Human Resource Management	Risk Management
Identity Management	Service Continuity
Incident Management & Control	Technology Management
Knowledge & Information Mgmt.	Vulnerability Analysis & Resolution

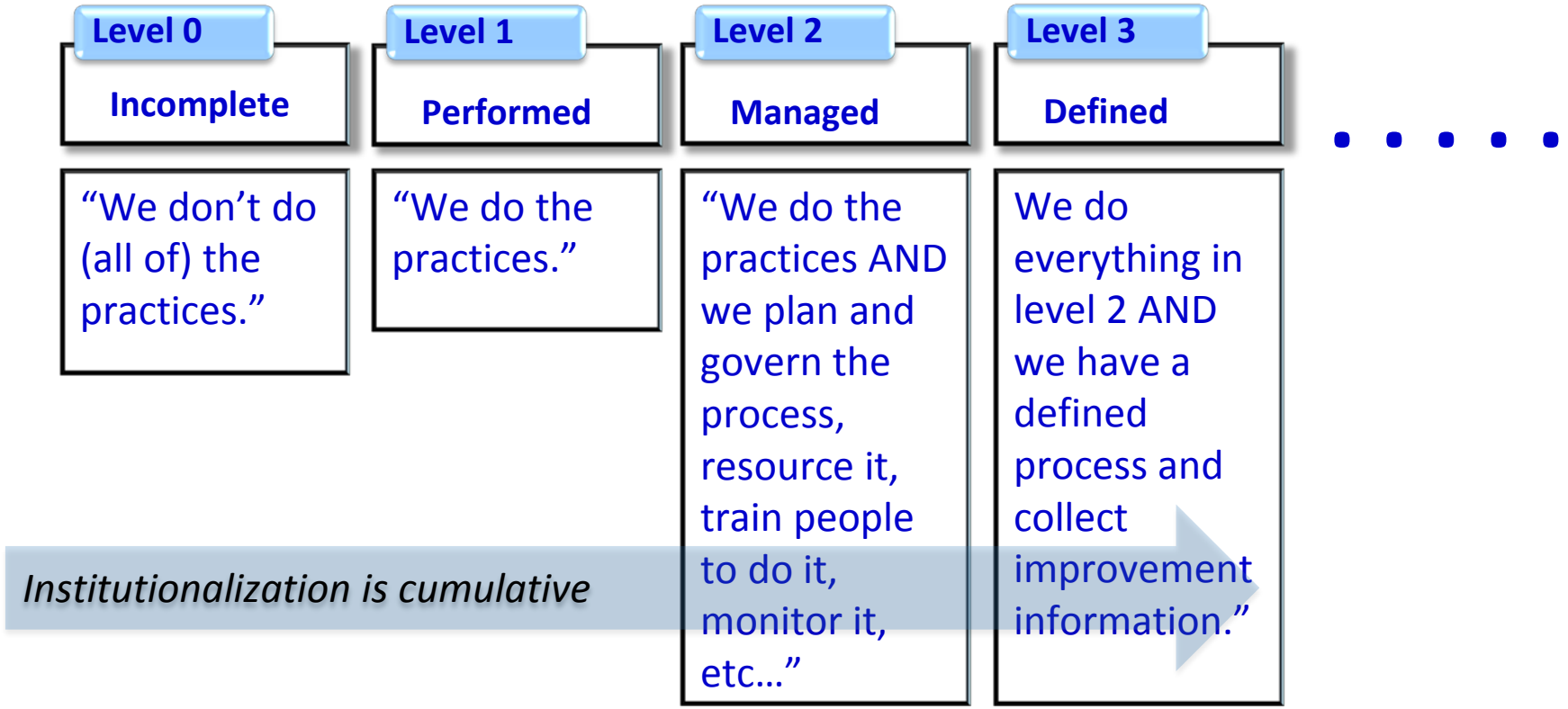
CMM Example: CERT-RMM

Consider the **Incident Management and Control (IMC)** domain from CERT-RMM:

- *Goal 1: Establish the IMC process*
- *Goal 2: Detect events*
- *Goal 3: Declare incidents*
- *Goal 4: Respond to and recover from incidents*
- *Goal 5: Establish incident learning*



CMM Example: CERT-RMM



Benefits and Limitations of CMMs

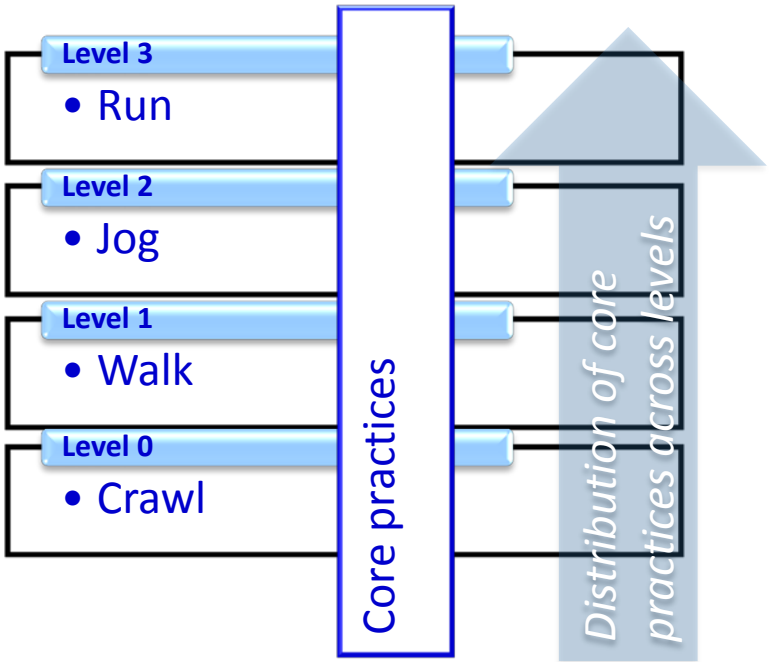
Benefits

- Provides for measurement of core competencies
- Provides for rigorous measurement of capability—the ability to retain core competencies under times of stress
- Can provide a path to quantitative measurement

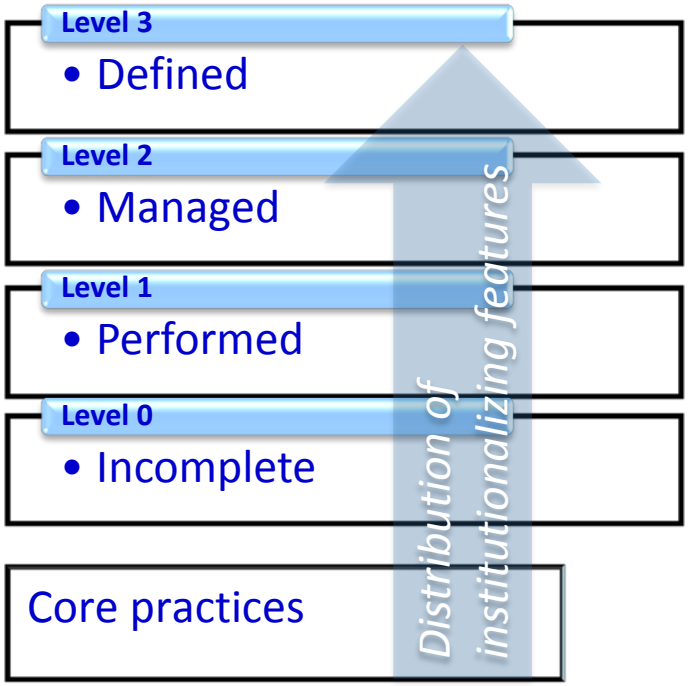
Limitations

- Sometimes difficult to understand and apply; high adoption cost
- “Maturity” may not translate into actual results
- Potential false sense of achievement: achieving high maturity in security practices may not mean the organization is “secure”

Compare: Progression vs CMM



Progression Model



Capability Model

Hybrid Maturity Model

Combines the best features of progression and capability maturity models

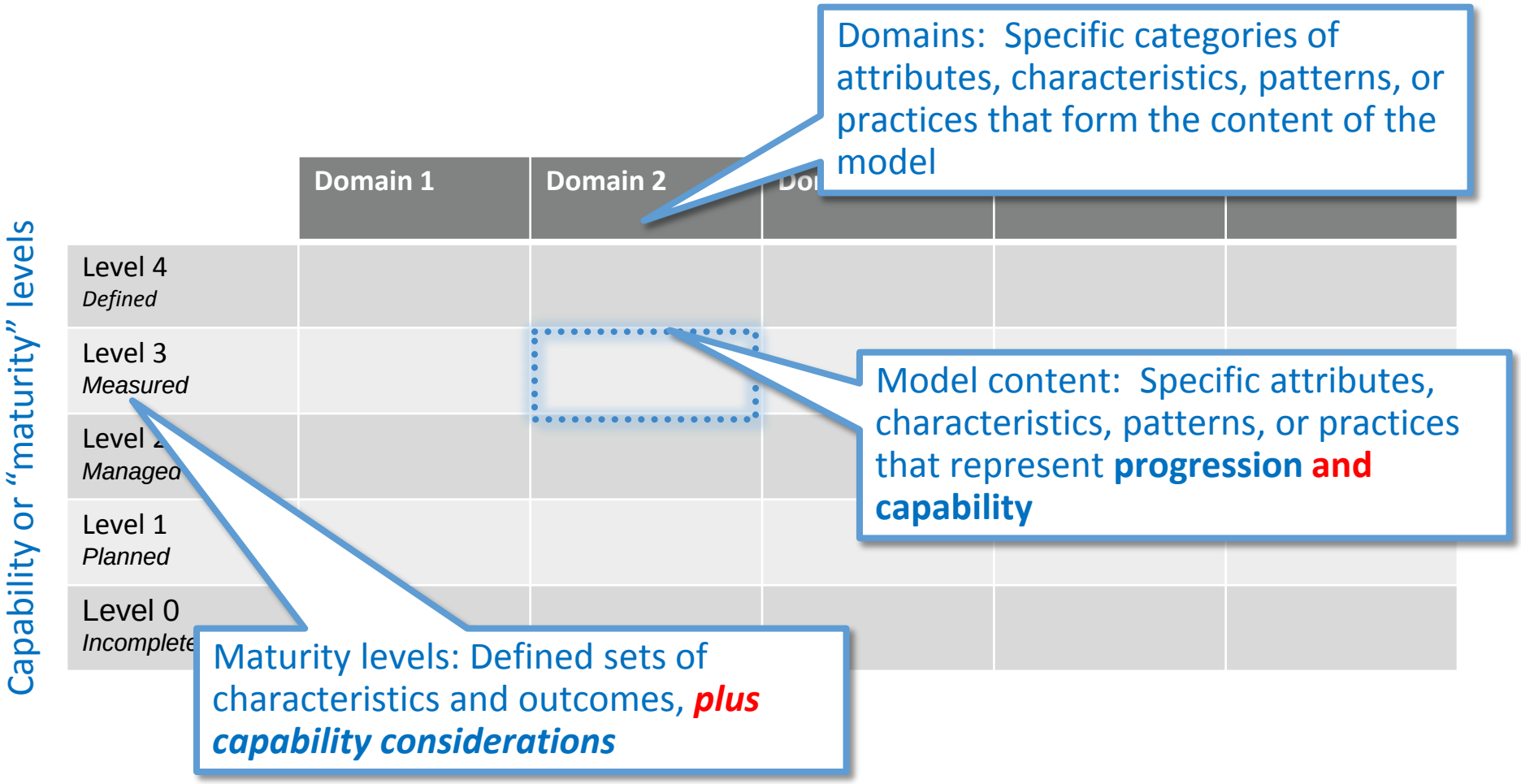
- Allows for measurement of evolution or achievement as in progression models
- Adds the ability to measure capability or institutionalization with the rigor of a CMM

Levels reflect both achievement and capability

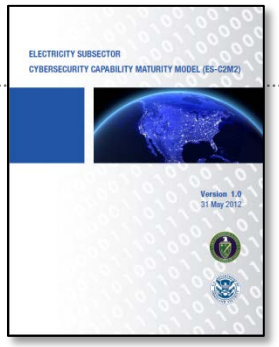
Transitions between levels:

- Similar to a capability model (i.e., describe capability maturity)
- Architecturally use the characteristics, indicators, attributes, or patterns of a progression model

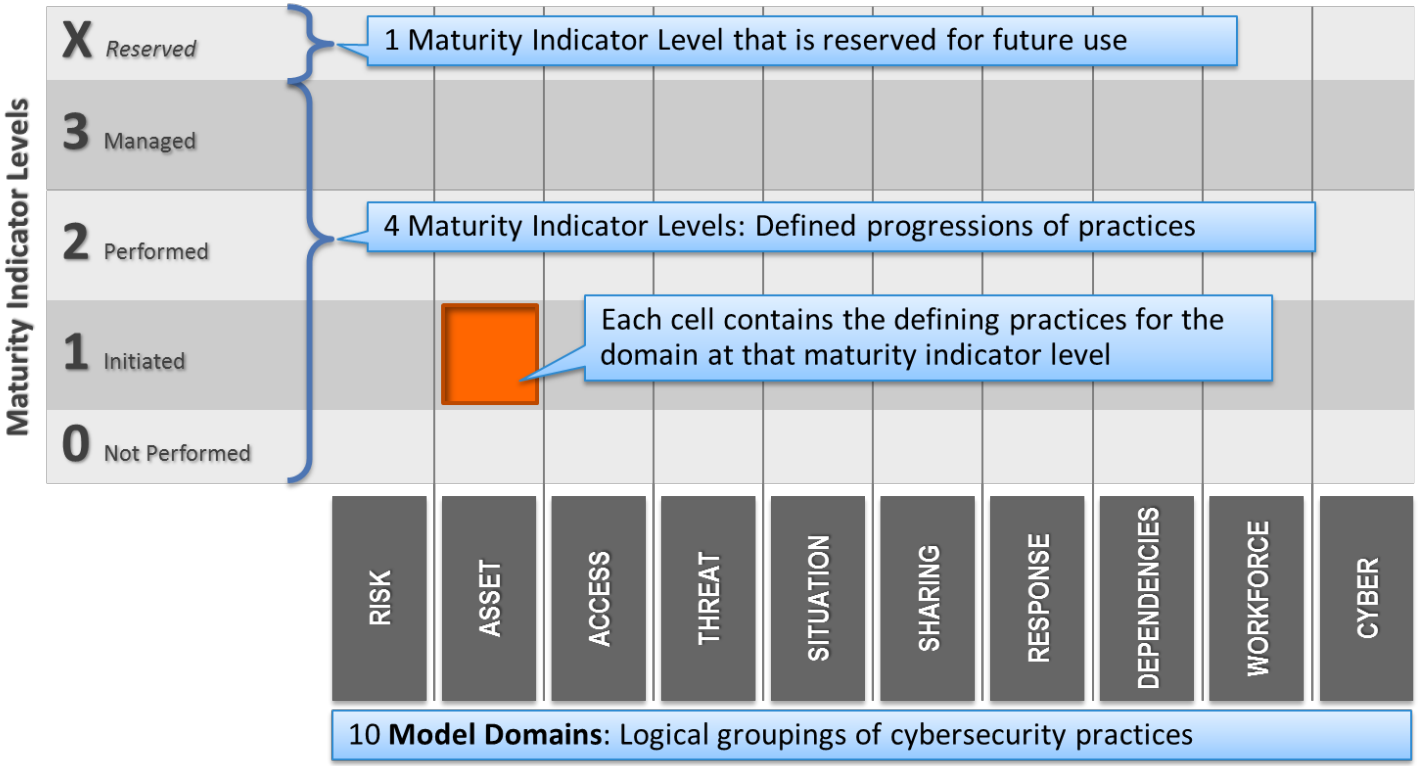
Hybrid Maturity Models



Hybrid Model Example: ES-C2M2



Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)



Benefits and Limitations of Hybrid Models

Benefits

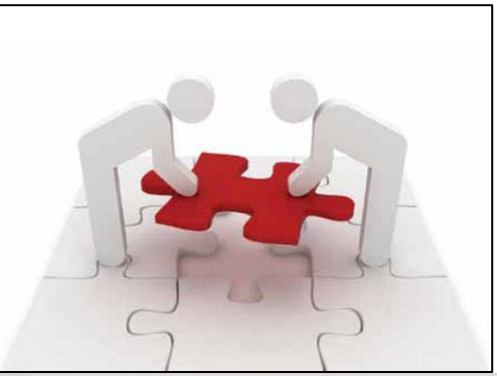
- Provides for easy measurement of core competencies as well as approximation of capability
- Can adapt easily to evolution of technologies and practices without sacrificing capability measurement
- Low adoption cost

Limitations

- "Maturity" concept is approximated; not as rigorous as CMM
- Combination of attributes with institutionalizing features at each level can be arbitrary

Closing Thoughts

- A few cautions
- Determining when and which type to use



First and Foremost

Have a clear understanding of your business objectives for using any type of improvement model

- How the model will meet these objectives

Understand how this initiative fits with others that are mainstream for the organization (not a new add-on)

Have visible sponsorship of executives and senior leaders who are essential for success

Have well-defined outcome measures that are regularly reported and reviewed

Have a plan and committed resources

A Few Cautions

Progression models may be easier to adopt but may not be sustainable (aka sticky)

Definitions of levels can be arbitrary

Measuring process performance and maturity is useful but may not be sufficient

Exercise care when using maturity models for specific purposes

When Does It Make Sense to Use Maturity Models?

Requirement for a structured approach

Demonstrated, measurable results based on an established body of knowledge

A defined roadmap from a current state to a desired state

An ability to monitor and measure progress, particularly in the presence of change

- Response to a strategic improvement or new product/new market objective

When Does It Make Sense to Use Maturity Models? *(cont.)*

Desire to answer these questions in a repeatable, predictable manner:

- How do I compare with my peers? (ability to benchmark)
- How can I determine how secure I am and if I am secure enough?
- How do I measure my current state? Characterize my desired state?
- What concrete actions do I need to take to improve? And in what order?
- How do I measure progress toward my desired state?
- How do I adapt to change?

Thank you for your attention…

References

Crosby, P. B. (1979). Quality is Free. New York: New American Library. ISBN 0-451-62247-2.

Nolan, R. L. (July 1973). "Managing the computer resource: A stage hypothesis". Comm. ACM 16 (7): 399–405. doi:10.1145/362280.362284

Humphrey, W. S. (March 1988). "Characterizing the software process: A maturity framework". IEEE Software 5 (2): 73–79. doi:10.1109/52.2014

Humphrey, W. S. (1989). Managing the Software Process. SEI series in software engineering. Reading, Mass.: Addison-Wesley. ISBN 0-201-18095-2

Paulk, Mark C.; Weber, Charles V.; & Curtis, Bill. The Capability Maturity Model: Guidelines for Improving the Software Process. Addison-Wesley Professional, 1994.

CMMI Overview. http://www.sei.cmu.edu/cmmi/ (2012).

Chris McClean and Khalid Kark, “Introducing the Forrester Information Security Maturity Model,” Forrester Research , July 27, 2010.

Caralli, Richard A.; Allen, Julia H.; & White, David W. *CERT® Resilience Management Model: A Maturity Model for Managing Operational Resilience.* Addison-Wesley, 2011.

Caralli, Richard A. *Discerning the Intent of Maturity Models from Characterizations of Security Posture.* Software Engineering Institute, Carnegie Mellon University, 2012. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=58922

Electricity Subsector Cybersecurity Maturity Model. Carnegie Mellon University, 2012. http://energy.gov/sites/prod/files/Electricity%20Subsector%20Cybersecurity%20Capabilities%20Maturity%20Model%20%28ES-C2M2%29%20-%20May%202012.pdf

Smart Grid: Tools and Methods. http://www.sei.cmu.edu/smartgrid/tools/ (2012).

Resilience Management. http://www.cert.org/resilience (2012).